

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

TECSEC, INC.,
Plaintiff,

V.

INTERNATIONAL BUSINESS
MACHINES CORPORATION, et al.,
Defendants.

)
)
)
)
)
)
)
)

1:10cv115 (LMB/TCB)

MEMORANDUM OPINION

Before the Court is defendant Adobe Systems Incorporated's Motion for Entry of its Proposed Claim Constructions and for Summary Judgment of Non-Infringement. [Dkt. No. 710] ("Motion for Summary Judgment"). For the reasons that follow, the motion for entry of Adobe's proposed claim constructions will be granted in part and the motion for summary judgment of non-infringement will be granted.

I. BACKGROUND

TecSec, Inc. (“TecSec” or “plaintiff”) is the owner of United States Patents Nos. 5,369,702 (the “702 Patent”), 5,680,452 (the “452 Patent”), 5,717,755 (the “755 Patent”), and 5,898,781 (the “781 Patent”).¹ Because all four patents address features of what the written description describes as a “Distributed Cryptographic Object Method” (“DCOM”), for the purposes of this litigation the four patents are collectively referred to as the “DCOM Patents.”²

¹ The '452 Patent and '755 Patent are direct continuations of the '702 Patent, and the '781 Patent is a direct continuation of the '755 Patent.

² TecSec also owns, and alleged that Adobe infringed, United States Patent No. 6,694,433, directed to an “XML Encryption Scheme” (the “XML Patent”). While this litigation has been pending, TecSec filed for supplemental examination of the XML Patent and the Patent Office issued a “Final Rejection” of all asserted claims of that patent. Although that decision was termed a “final” rejection, TecSec is currently in the process of appealing the rejection of the

TecSec alleges that Adobe Acrobat (“Acrobat”), a piece of software made by defendant Adobe Systems, Inc. (“Adobe” or “defendant”) infringes the DCOM Patents.

A. Encryption Basics

Because the DCOM Patents describe a method for securing digital objects using encryption, some background on encryption is helpful to understanding the claimed invention. Encryption is the process whereby original data, referred to as “plaintext,” can be transformed into encoded data, referred to as “ciphertext.” Charles P. Pfleeger & Shari Lawrence Pfleeger, *Security in Computing* 35-37 (Pearson Education, Inc. 3d ed. 2003). Encrypting data helps to prevent unauthorized users from accessing that data.

Digital files can be encrypted using encryption “keys.” Id. Like physical keys for physical locks, encryption keys can be used to “lock” data so that unauthorized users cannot access it, and also allow authorized users to “unlock” the data. Id. at 37. The encryption key is applied to the plaintext message pursuant to an encryption algorithm, resulting in ciphertext. Id. An authorized user can then decrypt the ciphertext to gain access to the plaintext. Id. In the simplest form of key-based encryption, referred to as a “symmetric key” system, the key used to encrypt the plaintext information is also used to decrypt the ciphertext. Id. The standard housekey system is a physical symmetric key system, in that the same key is used to both lock and unlock the door. Systems which use passwords, secret phrases which an authorized user must enter to gain access to the information, also tend to be symmetric key systems. In more complicated encryption systems, a different key is used to encrypt the plaintext than is used to decrypt the ciphertext. Id. Those systems are referred to as “asymmetric key” systems because

XML Patent to the Patent Trial and Appeal Board, Status Report Regarding U.S. Patent No. 6,694,433 [Dkt. No. 758], and has agreed to drop its claims against Adobe involving the XML Patent and to proceed against Adobe on an accelerated schedule regarding the DCOM Patents.

different keys are used to encrypt and decrypt. Id. The equivalent physical system would have one key used to lock a door, but a different key used to unlock that same door. See id.

Digital certificates, which are particularly relevant to the present action, use an asymmetric key system to protect information. A digital certificate is “similar to a passport or driver’s license” in that it can be used with confidence to identify an individual or organization. Umesh H. Rao & Umesha Nayak, *The InfoSec Handbook* 172 (Apress Media 2014). The certificate is issued by a trusted third-party “certificate authority” which verifies the identity of the individual before the certificate is issued. Id. at 171-72. Digital certificates can be used to secure data through public key cryptography, which is an asymmetric key system. Id. at 170-71. The certificate authority issues an individual a public key and a private key. The public key can be accessed by anyone, but the private key is only available to the individual. Id. Data encrypted with an individual’s public key may only be decrypted with that individual’s private key, and data encrypted with an individual’s private key may only be decrypted with that individual’s public key. Id. Accordingly, the public key from an individual’s digital certificate can be used to encrypt a document. Because only the individual has the private key, which is the only way to decrypt the document, the sender can be sure that the content of the document will remain secure and will only be seen by the intended recipient. See id. “An individual or organization may have any number of certificates issued by different [certificate authorities].” Id. at 172.

B. The DCOM Patents

The DCOM Patents describe a method and system which allows a user to flexibly secure computer objects by encrypting a first object, nesting the encrypted first object into a second object, and then encrypting the second object. ‘702 Patent col. 4 lines 14-34. The encryption and nesting process may be repeated any number of times, and each encryption iteration can use a

different encryption key. Id. col. 11 lines 40-55. As a result, users can securely transmit a single object containing multiple other objects, allowing recipients to decrypt only those objects to which each particular recipient is entitled access. Id. In the context of a company, for example, “[e]very employee would receive the single encrypted file, but they would only be able to unravel the portions that corresponded to them and acquire no knowledge of other existing embedded encrypted objects.” Id. col. 11 lines 44-48. Figure 3, which illustrates the process at a high level, shows “an encrypted object that contains a web of embedded encrypted objects nested within the other encrypted objects[:.]”

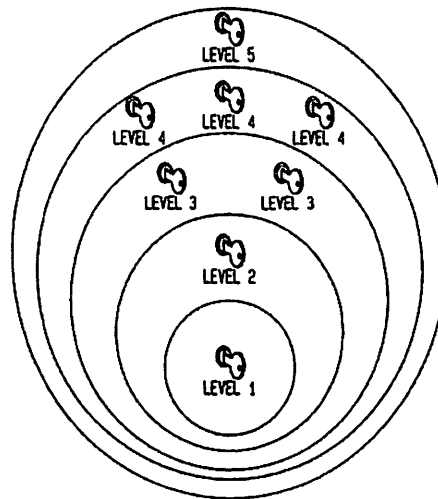


FIG. 3

Id. col. 11 lines 18-30. The object in Figure 3 “contains ten embedded encrypted objects at five various levels. The encrypted object embedded in level 5 was embedded in an object in level four, level four objects in level 3 and so on.” Id.

In addition to multi-level encryption, the DCOM Patents use labels to provide protection:

[A] sending user can specify label conditions that limit access to the transmitted message. For example, many people within a company may have the key necessary to read a data file that a sender may transmit from his computer terminal to other terminals at another

site within his company. The sender may, however, wish to restrict reception to those persons present at a particular terminal. By employing a secure labelling technique in addition to encryption, the sender can be assured that people having the correct key to decrypt the message but working at different terminals will not receive or be allowed to access the communication.

Id. col. 2 lines 44-56. Accordingly, after encryption a user may select a label for an object, and the label is attached to the object. Id. Claim 1 of the '702 Patent illustrates the labelling and encryption systems working together to ensure security:

1. A method for providing multi-level multimedia security in a data network, comprising the steps of:

- A) accessing an object-oriented key manager;
- B) selecting an object to encrypt;
- C) selecting a label for the object;
- D) selecting an encryption algorithm;
- E) encrypting the object according to the encryption algorithm;
- F) labelling the encrypted object;
- G) reading the object label;
- H) determining access authorization based on the object label; and
- I) decrypting the object if access authorization is granted.

Id. col. 12 lines 1-15. TecSec admits that “[c]laim 1 of the ‘702 [P]atent is exemplary.” TecSec’s Brief in Opposition to Adobe Systems Inc.’s Proposed Claim Constructions and Motion for Summary Judgment of Non-Infringement [Dkt. No. 741] (“MSJ Opp’n”) at 8.

C. Adobe Acrobat

“Adobe offers a family of software applications under the name Acrobat that are used to view, create, manipulate, print and manage PDF documents.” Declaration of Marc Kaufman [Dkt. No. 712] Att. 1 (“Kaufman Dec.”) ¶ 4.³ PDF, which stands for “portable document format,” is an open source standard file format which allows a document to be electronically

³ TecSec’s expert, Dr. Mark Jones, does not offer any opinions regarding the general PDF standard or describing its general operation; however, Dr. Marc Kaufman, Adobe’s Fed. R. Civ. P. 30(b)(6) witness, does provide such background and TecSec does not dispute Dr. Kaufman’s description. Accordingly, the basic structure of a PDF document is not in dispute.

displayed “with the same form, font and layout as it would if it were printed, regardless of the particular software, hardware or operating system used to display the document.” Id. ¶ 2. To view a document stored in the PDF format, a user must have a program that can interpret and display a PDF document (a “PDF reader”) installed on her computer. Id. ¶ 4. Because PDF is an open file format, any company or programmer could create their own PDF reader. Id. Acrobat is Adobe’s implementation of a PDF reader. Id. Successive versions of Acrobat have been introduced as the PDF standard evolved. See id. ¶ 5.

Understanding the PDF standard is necessary to understand how Acrobat functions. A PDF document consists of four components: objects, file structure, document structure, and content streams. Id. ¶ 6. The components are shown below:

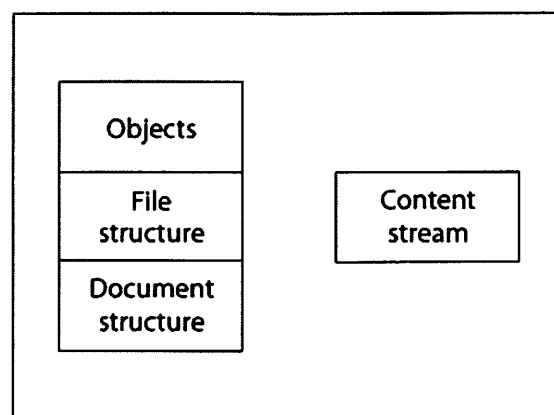
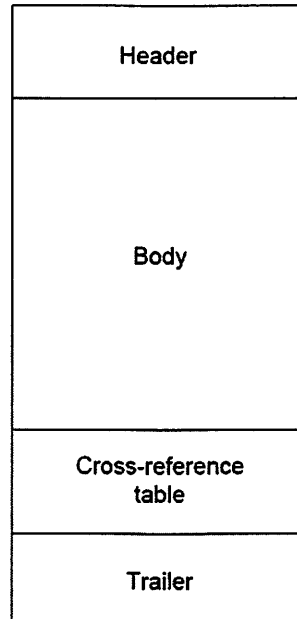


Figure 1 – PDF Components

Id. Objects “build” most of the elements that a user sees when a PDF document is opened. There are seven different types of objects. Id. ¶¶ 6-7. Relevant to this civil action is the “dictionary” type of object, which is a table containing pairs of objects.⁴ Id. ¶ 7f. The document structure

⁴ “A dictionary object is an associative table containing pairs of objects, known as the dictionary’s entries. The first element of each entry is the key and the second element is the

“consists of a number of data structures that define the structure of the document itself, such as which objects belong on a given page.” Id. ¶ 9. Content streams contain instructions describing the appearance of a page in a PDF document. Id. ¶ 9. File structures “determine[] how objects are stored in a PDF document and how they are accessed.” Id. ¶ 8. The file structure for a PDF document is shown below:



Id. The “body” contains all of the objects that make up the document’s content, the “cross-reference table” identifies the locations of objects within the document, and the “trailer” specifies the location of the cross-reference table and includes a “trailer dictionary” which organizes references to important parts of the file. Id.

value.” Id. ¶ 7f. In that manner, the structure of a dictionary object is the same as the structure of an English language dictionary, where a word is the “key” and the word’s definition is the “value.” A dictionary object uses that flexible structure “to collect and tie together the attributes of a more complex data structure, such as a font or a page of a document[.]” Id. “[E]ach entry in the dictionary specif[ies] the name and value of an attribute of the more complex structure.” Id.

A PDF document may have other files, including other PDF documents, attached to it. Id.

¶ 11. A file which is attached to a PDF document is held within the body section of the PDF document, and is stored like any other content. Id. ¶¶ 12-13. A user can see and select any attached files when the PDF document is opened in Acrobat. Id. If the user selects and tries to open an attached file, the file “is opened like any other file on a computer.” Id. ¶ 13. For example, if a Microsoft Word file is attached to a PDF document and the user attempts to open the Microsoft Word file, the file will be opened by Microsoft Word. Id. Similarly, when a user attempts to open a PDF document attached to another PDF document, the attached PDF document will be opened in another session of Acrobat. Id. ¶ 13. If the attached PDF document also has attachments, those attachments are treated in the same way. Id.

In addition, a PDF document may also contain metadata. Metadata is “global information about the document (as opposed to its content or structure),” and may include “the document’s title, author, and creation and modification dates.” PDF Reference, Adobe Portable Document Format Version 1.7 at 843 (Adobe Systems Incorporated 6th ed. 2006).⁵ Metadata is used to “assist in cataloguing and searching for documents in external databases.” Id. Metadata is stored either within a dictionary in the trailer of the document, id., or within the body of the document. Id. at 845-47.

D. Encrypting a PDF Document Using Adobe Acrobat

The parties agree that Acrobat has the capability to encrypt a PDF document. Kaufman Dec. ¶ 18; Declaration of Mark T. Jones, Ph.D [Dkt. No. 738] (“Jones Dec.”) ¶¶ 22-23. When using Acrobat there are three options for encryption: (1) encrypt everything in the file (including

⁵ Available at http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/pdf_reference_1-7.pdf.

metadata and any attachments); (2) encrypt everything except the metadata; and (3) encrypt only the attachments. Jones Dec. ¶ 36. One method for encrypting a PDF document is to use a password. Id. ¶¶ 40, 45. If the document is encrypted using a password, the document can be protected by both an “owner” password, which gives a person unrestricted access to the document and any function allowed by Acrobat, and a “user” password, with which the owner can limit what a user may do once he has access to the file. Declaration of Michael A. Oakes [Dkt. No. 737] Ex. 2 (“Kaufman 30(b)(6) Dep.”) at 22-25. For example, the owner of a document can use Acrobat to allow those who enter the user password only to read but not to print the document. If a person enters the owner password, however, she can use any function such as saving, printing, editing, etc. In essence, creating an owner and user password creates two “tiers” of use for a document. When the owner of a PDF document selects the option to encrypt that PDF document, the owner is prompted to create both passwords.

After a PDF document has been encrypted, information necessary to decrypt the document is stored in the trailer section of the file in a special object called the “encryption dictionary.” See, e.g., id. at 17; Kaufman Dec. ¶ 22; Jones Dec. ¶ 68. “[T]he encryption dictionary is not visible to users, but is part of the internal structure of the document.” Kaufman Dec. ¶ 22. If the PDF document is password-secured, the encryption dictionary includes values which are used to test the owner and user password (the “O key” and “U key,” respectively) to determine if the recipient entering the password is authorized to access the document.⁶ Kaufman 30(b)(6) Dep. at 17. The encryption dictionary is not generated immediately after the owner of the PDF document creates the passwords. See id. at 14. Instead, Acrobat automatically creates

⁶ The encryption dictionary includes other values as well, including the permission settings and the algorithm used to encrypt the PDF document. Jones Dec. ¶ 68.

the O key, U key, and encryption dictionary only after the user chooses to “save” the PDF document. See e.g. id. at 14-17. If the user does not save the document, the encryption dictionary does not exist at all. See id. In other words, the encryption dictionary does not exist until the user selects “save.” Moreover, neither the owner nor the user passwords themselves are directly included in the encryption dictionary, only the values assigned to those passwords are included in the encryption dictionary. Id.

A PDF document may also be encrypted using digital certificates. Jones Dec. ¶¶ 40, 45. The process for using digital certificates to encrypt a PDF document is slightly different than the process for using a password. Once the user decides which parts of the PDF document are to be encrypted,⁷ the user selects the digital certificates of the recipients to whom the PDF document will be sent.⁸ Kaufman 30(b)(6) Dep. at 45. The user can also sort the recipients into groups, and can restrict the functions available to each group. Id. at 49-50. Similar to password security, however, encryption of the PDF document and creation of the encryption dictionary do not occur until after the user chooses to save the document. Id. at 54, 63. When the user saves the document, Acrobat generates a random number, referred to as a “file key,” which is used to encrypt the PDF document.⁹ Id. at 51-52, 61. The file key is encrypted for each recipient with that recipient’s public key. Id. at 52. Acrobat then automatically creates the encryption dictionary, and the encrypted file keys are inserted into the encryption dictionary along with

⁷ As with password security, Acrobat can encrypt either everything in the file (including metadata and any attachments), everything except the metadata, or only the attachments using certificate security.

⁸ The digital certificates may be stored with Adobe, or on the user’s hard drive, or on a storage device attached to the computer. Id. at 46.

⁹ Once the file key is generated, Acrobat follows the same process to encrypt the PDF document with the certificate as it does when encrypting a PDF document using password security. Id. at 61.

identifiers for the related digital certificates (although not the certificates themselves). Id. at 52-54. By grouping recipient certificates together and assigning those groups functions that they can perform, the owner of a PDF document may also use certificate security to create tiers of use for a document.

II. PROCEDURAL HISTORY

TecSec originally filed this action against thirteen defendants asserting infringement of the DCOM Patents as well as other patents not relevant to the current motion. To make the litigation manageable, IBM was selected as the first defendant against which the litigation would proceed. In that litigation, several claim terms, including “multimedia” and “multi-level . . . security,” were construed, IBM was granted summary judgment on a finding that it did not infringe any asserted patent, and the Federal Circuit affirmed. TecSec, Inc. v. IBM et al., 466 Fed. App’x 882 (Fed. Cir. Jan. 18, 2012). TecSec and IBM subsequently settled.

Rather than continue to prosecute its claims against the remaining defendants, TecSec stipulated that it could not prove infringement of the DCOM Patents against any defendant under the construction of “multimedia,” and could not prove infringement of the DCOM Patents against Paypal, Inc. (“PayPal”) under the construction of “multi-level . . . security.” Accordingly, judgment was entered against TecSec, and TecSec appealed. At TecSec’s request, the litigation was stayed pending the outcome of the appeal. The Federal Circuit affirmed the construction of “multi-level . . . security,” but reversed the construction of “multimedia.” TecSec, Inc. v. IBM et al., 731 F.3d 1336, 1345-46 (Fed. Cir. 2013). Defendants filed a petition for a writ of certiorari, and the stay of this litigation was continued while the petition was pending. After the petition was denied on June 2, 2014, and the mandate was returned, TecSec agreed to proceed against Adobe under only the DCOM Patents on an accelerated schedule.

III. DISCUSSION

TecSec alleges that Acrobat infringes claims 1, 4, 8, and 9 of the ‘702 Patent, claim 1 of the ‘452 Patent, claim 1 of the ‘755 Patent, and claims 1, 3, 14, and 15 of the ‘781 Patent (collectively, the “asserted claims”). Adobe moves for summary judgment of non-infringement, centering its arguments on the “multi-level . . . security” and “labelling” limitations in the claims, as well as presenting arguments regarding the object-oriented key manager. Motion for Summary Judgment Att. 1 (“MSJ Br.”). Although TecSec asserts in its pleading that “Acrobat [i]nfringes [t]he DCOM Patents,” MSJ Opp’n at 8, TecSec has not moved for summary judgment of infringement, despite receiving the opportunity to do so. See November 10, 2014 Order [Dkt. No. 724].

The asserted claims are set forth below.¹⁰ Claim 4 of the ‘702 Patent and claim 3 of the ‘781 Patent depend on unasserted claims; because dependent claims include the limitations of the claims on which they depend, the limitations of the unasserted claims must also be addressed.

‘702 Patent	
Claim 1	“A method for providing multi-level multimedia security in a data network, comprising the steps of: A) accessing an object-oriented key manager; B) selecting an object to encrypt; C) selecting a label for the object; D) selecting an encryption algorithm; E) encrypting the object according to the encryption algorithm; F) labelling the encrypted object;

¹⁰ The asserted claims are exceptionally broad, and provide little detail regarding how a person of ordinary skill in the art would implement the claimed invention. The lack of detail renders the claims remarkably abstract – “[i]ndeed, it is difficult to conceive of broader terms with which the idea of” multi-level encryption “could be described.” Amdocs (Israel) Ltd. v. Openet Telecom, Inc., No. 1:10cv910, 2014 WL 5430956, at *6 (E.D. Va. Oct. 24, 2014) (invalidating claims to correlating two network records under 35 U.S.C. 101 for being drawn to an unpatentable abstract idea). As validity is not presently before the Court, however, there is no cause to consider validity issues at this time.

	<p>G) reading the object label; H) determining access authorization based on the object label; and I) decrypting the object if access authorization is granted.”</p>
Claim 4	<p>“[The method of claim 1, further comprising the step of embedding the encrypted object in a second object after labelling the encrypted object, and], further comprising the steps of: A) selecting a second label for the second object; B) selecting an encryption algorithm; C) encrypting the second object; and D) labelling the second encrypted object with a second object label.”</p>
Claim 8	<p>“A system for providing multi-level multimedia security in a data network, comprising: A) digital logic means, the digital logic means comprising: 1) a system memory means for storing data; 2) an encryption algorithm module, comprising logic for converting unencrypted objects into encrypted objects, the encryption algorithm module being electronically connected to the system memory means for accessing data stored in the first system memory; 3) an object labelling subsystem, comprising logic means for limiting object access, subject to label conditions, the object labelling subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object labelling subsystem being further electronically connected to the encryption algorithm module to accept inputs from the encryption module; 4) a decryption algorithm module, comprising logic for converting encrypted objects into unencrypted objects, the decryption algorithm module being electronically connected to the system memory means for accessing data stored in the system memory means; and 5) an object label identification subsystem, comprising logic for limiting object access, subject to label conditions, the object label identification subsystem being electronically connected to the system memory means for accessing data stored in the system memory means and the object label identification subsystem being further electronically connected to the decryption algorithm module to accept inputs from the decryption algorithm module; B) the encryption algorithm module working in conjunction with the object labelling subsystem to create an encrypted object such that the object label identification subsystem limits access to an encrypted object.”</p>
Claim 9	<p>“The system of claim 8, wherein the digital logic means further comprises means for embedding a first object within a second object.”</p>

‘452 Patent	
Claim 1	“A method for providing multi-level multimedia security in a data network,

	comprising: a) accessing an object-oriented key manager; b) selecting a first object to encrypt; c) selecting a first label for the first object; d) encrypting the first object; e) labelling the encrypted first object; f) displaying the first label as a header array; g) reading the first object label; h) determining access authorization based on the first object label; and i) decrypting the first object if access authorization is granted.”
--	--

‘755 Patent	
Claim 1	“A method for providing multi-level multimedia security in a data network, comprising: A) accessing an object-oriented key manager; B) selecting a first object to encrypt; C) selecting a first label for the first object; D) selecting an encryption algorithm; E) encrypting the first object according to the encryption algorithm; F) labelling the encrypted first object according to the encryption algorithm; G) reading the first object label; H) determining access authorization based on the first object label; and I) allowing access to the first object only if access authorization is granted.”

‘781 Patent	
Claim 1	“A method for providing multi-level multimedia security in a data network, comprising: A) accessing an object-oriented key manager; B) selecting a first object to encrypt; C) selecting a first label for the first object; D) selecting an encryption algorithm; E) encrypting the first object according to the encryption algorithm; F) labelling the encrypted first object; G) reading the first object label; H) determining access authorization based on the first object label; and I) allowing access to the first object only if access authorization is granted.”
Claim 3	“[The method of claim 1, further comprising embedding the encrypted first object in a second object after labeling the encrypted first object, and] further comprising: A) selecting a second label for the second object; B) selecting an encryption algorithm; C) encrypting the second object; D) labelling the encrypted second object with a second object label.”

Claim 14	<p>“A system for providing multi-level multimedia security in a data network, comprising:</p> <ol style="list-style-type: none"> 1) a system memory for storing data; 2) an encryption algorithm module, comprising logic for converting unencrypted objects into encrypted objects, the encryption algorithm module being disposed to access data stored in the system memory; 3) an object labelling subsystem, comprising logic for applying label conditions to an object, the object labelling subsystem being disposed to access data stored in the system memory and the object labelling subsystem being further disposed to accept inputs from the encryption of the algorithm module; 4) a decryption algorithm module, comprising logic for converting encrypted objects into unencrypted objects, the decryption algorithm module being disposed to access data stored in the system memory means; and 5) an object label identification subsystem, comprising logic for limiting object access, according to the label conditions, the object label identification subsystem being disposed to access data stored in the system memory and the object label identification subsystem being further disposed to accept inputs from the decryption algorithm module; 6) wherein the encryption algorithm module and the object labelling subsystem together create an encrypted object such that the object label identification subsystem limits access to the encrypted object.”
Claim 15	<p>“The system of claim 14, wherein the data processor further comprises embedding logic for embedding a first object within a second object.”</p>

A. Standard of Review

Summary judgment is appropriate where the record demonstrates “that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c). A genuine issue of material fact exists “if the evidence is such that a reasonable jury could return a verdict for the nonmoving party.” Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 247-48 (1986).

The Court must view the record in the light most favorable to the nonmoving party, see Bryant v. Bell Atl. Md., Inc., 288 F.3d 124, 132 (4th Cir. 2002); however, the “mere existence of a scintilla of evidence in support of the [nonmovant’s] position will be insufficient; there must be evidence on which the jury could reasonably find for the [nonmovant].” Anderson, 477 U.S. at

252; see also Othentec Ltd. v. Phelan, 526 F.3d 135, 140 (4th Cir. 2008); TecSec, Inc. v. Int'l Bus. Machines Corp., 763 F. Supp. 2d 800, 804-05 (E.D. Va. 2011) aff'd, 466 F. App'x 882 (Fed. Cir. 2012). When relying on expert testimony, “[a] party does not manufacture more than a merely colorable dispute by submitting an expert declaration that something is black when the moving party’s expert says it is white; there must be some foundation or basis for the opinion.” Invitrogen Corp. v. Clontech Labs., 429 F.3d 1052, 1080 (Fed. Cir. 2005).

B. Claim Construction

“The first step of the infringement analysis is claim construction,” Nazomi Comm’ns, Inc. v. Nokia Corp., 739 F.3d 1339, 1343 (Fed. Cir. 2014), an issue of law for determination by the Court, Markman v. Westview Instruments, Inc., 517 U.S. 370, 387 (1996), which “begins with the language of the claim.” Power Integrations, Inc. v. Fairchild Semiconductor Intern., Inc., 711 F.3d 1348, 1360 (Fed. Cir. 2013). The general rule is that the words of the claim are “given their ordinary and customary meaning as understood by a person of ordinary skill in the art when read in the context of the specification and prosecution history.” Thorner v. Sony Computer Entm’t, 669 F.3d 1362, 1365 (Fed. Cir. 2012). The “primary focus in determining the ordinary and customary meaning of a claim limitation is to consider the intrinsic evidence of record, viz., the patent itself, including the claims, the specification and, if in evidence, the prosecution history, from the perspective of one of ordinary skill in the art.” Atofina v. Great Lakes Chem. Corp., 441 F.3d 991, 996 (Fed. Cir. 2006) (citing Phillips v. AWH Corp., 415 F.3d 1303, 1312-17 (Fed. Cir. 2005) (en banc)).

One of “only two exceptions” to the general rule that words in a claim should be given their plain meaning to one of ordinary skill is “when a patentee sets out a definition and acts as his own lexicographer.” Thorner, 669 F.3d at 1365. “To act as its own lexicographer, a patentee

must ‘clearly set forth a definition of the disputed claim term’ other than its plain and ordinary meaning.” Id. (quoting CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366 (Fed. Cir. 2002)). For example, the Federal Circuit has found that a patentee acted as his own lexicographer to define the term “multiple embossed” when “the specification stated: ‘Multiple embossed’ means two or more embossing patterns are superimposed on the web to create a complex pattern of differing depths after embossing.” Id. (quoting 3M Innovative Props. Co. v. Avery Dennison Corp., 350 F.3d 1365, 1369 (Fed. Cir. 2003)). Although “claims must be read in view of the specification, of which they are a part,” Philips, 415 F.3d at 1315 (internal quotation marks omitted), limitations from the specification may not be read into the claims. Id. at 1320.

The second exception to the general rule is “when a patentee disavows the full scope of a claim term either in the specification or during prosecution,” id. at 1365; however, “[a]bsent a clear disavowal in the specification or the prosecution history, the patentee is entitled to the full scope of its claim language.” Id. at 1366 (quoting Home Diagnostics, Inc. v. LifeScan, Inc., 381 F.3d 1352, 1358 (Fed. Cir. 2004)). “Mere criticism of a particular embodiment encompassed in the plain meaning of a claim term is not sufficient to rise to the level of a clear disavowal.” Id.

In construing a claim term, the Court begins with the language of the claims themselves. Philips, 415 F.3d at 1314. “[T]he context in which a term is used in the asserted claim can be highly instructive,” and “claim terms are normally used consistently throughout the patent.” Id. “Other claims of the patent in question, both asserted and unasserted, can . . . be valuable sources of enlightenment as to the meaning of a claim term.” Id. Accordingly, “[d]ifferences among claims can . . . be a useful guide in understanding the meaning of particular claim terms. For example, the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.” Id. at 1314-

15 (citations omitted). In particular, “‘claim differentiation’ refers to the presumption that an independent claim should not be construed as requiring a limitation added by a dependent claim,” Curtiss-Wright Flow Control Corp. v. Velan, Inc., 438 F.3d 1374, 1380 (Fed. Cir. 2006), though the doctrine can be overridden if the inventor provides an express definition. TecSec, Inc. v. Intern. Bus. Mach. Corp., 731 F.3d 1336, 1345 (Fed. Cir. 2013).

When performing claim construction, the Federal Circuit has expressed a preference for intrinsic evidence over dictionaries or other extrinsic evidence. “Intrinsic evidence . . . is a more reliable guide to the meaning of a claim term than are extrinsic sources like technical dictionaries, treatises, and expert testimony.” Chamberlain Grp., Inc. v. Lear Corp., 516 F.3d 1331, 1335 (Fed. Cir. 2008). “[T]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.” Power Integrations, 711 F.3d at 1361 (quoting Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996)). “Although definitions based on dictionaries, treatises, industry practice, and the like are often important aids in interpreting claims, they may not be ‘used to contradict claim meaning that is unambiguous in light of the intrinsic evidence.’” ArcelorMittal France v. AK Steel Corp., 700 F.3d 1314, 1320 (Fed. Cir. 2012) (quoting Phillips, 415 F.3d at 1312-17).

“The district court . . . has an obligation . . . to carefully consider, and independently decide, the issues in the case.” LSI Indus., Inc. v. ImagePoint, Inc., 279 F. App’x 964, 969 (Fed. Cir. 2008). This includes an “independent obligation to determine the meaning of the claims, notwithstanding the views asserted by the adversary parties.” Bancorp Servs., LLC v. Sun Life Assur. Co., 687 F.3d 1266, 1274 (Fed. Cir. 2012) (quoting Exxon Chem. Patents, Inc. v. Lubrizol Corp., 64 F.3d 1553, 1555 (Fed. Cir. 1995)). “When the parties present a fundamental dispute

regarding the scope of a claim term, it is the court's duty to resolve it." O2 Micro Intern. Ltd. v. Beyond Innovation Tech. Co., Ltd., 521 F.3d 1351, 1362 (Fed. Cir. 2008).

The Court previously construed "object" to mean "any distinct, separate entity" and "multi-level . . . security" to mean "security achieved when encrypted objects are nested within other objects which are also encrypted, possibly within other objects, resulting in multiple layers of encryption." Accordingly, those constructions are not in dispute. The parties dispute five terms. By proposing single constructions across all DCOM Patents, TecSec and Adobe agree that each claim term should have a single definition.

1. "selecting a label for the object"

The parties did not propose a construction for the clause "selecting a label for the object." At oral argument, the Court advised the parties that it viewed the claim term as potentially dispositive, depending on whether "selecting a label" includes "creating a label" or "selecting the components that go into a label." Transcript of Jan. 23, 2015 Hearing [Dkt. No. 769] ("MSJ Oral Argument Transcript") at 3-4, 7. Accordingly, the parties were given the opportunity to brief the issue. Id. at 3, 5, 7, 20. The parties advised that they did not believe that briefing was necessary, id. at 7, 20, but clearly dispute whether "selecting a label" includes "creating a label" or "selecting the components that go into a label." See id. at 3-8. As "the parties present a fundamental dispute regarding the scope of a claim term, it is the court's duty to resolve it." O2 Micro Intern. Ltd., 521 F.3d at 1362.

Claim 1, standing alone, does not provide much insight into a more precise definition of "selecting a label." The claim uses the term "selecting" three times ("selecting an object to encrypt," "selecting a label for the object," and "selecting an encryption algorithm"), but the claim does not provide any detail regarding what it means to "select." Of significance to the

infringement analysis, nothing in the claim clarifies whether the object, label, or algorithm must exist before they are selected or whether selecting includes actually creating the object, label, or algorithm.

Claim 1's dependent claims, however, provide some insight. Claim 2 adds to claim 1 "creating an object in an application prior to accessing the object-oriented key manager." That language clarifies that before an object can be selected, it must first be created.¹¹ Under the doctrine of claim differentiation, the addition of the "creating" step in claim 2 provides strong evidence that the "selecting" step in claim 1 does not include "creating." To read "selecting an object" to include "creating an object" would be to render the added step in claim 2 superfluous. Moreover, "claim terms are normally used consistently throughout the patent," Philips, 415 F.3d at 1314, therefore, the term "selecting" in "selecting an object" should have the same meaning when used in the claim term "selecting a label." Because there is no evidence that the inventor intended "selecting" to mean something different when dealing with an object rather than when dealing with a label or encryption algorithm, the language of the claims provides strong evidence that "selecting a label" does not include "creating a label."

The specification also forms part of the intrinsic evidence used in claim construction, Philips, 415 F.3d at 1315, and supports this analysis. Although the specification does not further refine "selecting a label," in each example where a user "[s]elects object(s) to [e]ncrypt," the user first "creates an object." '702 Patent col. 8 lines 1-4, col. 9 lines 11-14, and col. 10 lines 17-19. In addition, before a user "[s]elects object(s) to [p]review," the user "creates an encrypted

¹¹ Claim 13 similarly restricts claim 12.

object.” Col. 10 line 18 – col. 11 line 2. The written descriptions of the other patents in the DCOM family express the same difference between “selecting” and “creating.”¹²

Although limitations from the specification may not be read into the claims, the description of “labelling” in the specification, consistent with its use in the claims, indicates that the label is “selected” from, for example, a list of users or terminals which are allowed to see the message. Id. col. 2 lines 31-57. As described in the specification, “selecting a label” requires a user to actively choose a pre-existing label. In order for “the sender [to] be assured that people having the correct key to decrypt the message but working at different terminals will not receive or be allowed to access the communication,” id., the user must have pre-existing terminals from which to choose; and have the capability to actively choose which terminals can access the encrypted object.

Extrinsic evidence may also be relevant to claim construction. Philips, 415 F.3d at 1317-18. To the extent that it is necessary, extrinsic evidence provides further support for this construction of the meaning of “selecting.” A dictionary published during the same time as the initial application for the DCOM Patents defines “select” as “chosen from a number or group by fitness or preference.” Webster’s Third New International Dictionary 2058 (1993). From that standard definition, it is obvious that in order to be selected the selected item must first exist. Accordingly, the intrinsic and extrinsic evidence supports the conclusion that to “select[] a label for the object,” the label must have been created before the selection is made.

¹² ‘755 Patent col. 7 line 66 – col 8 line 2, col 9 lines 5-9, 39-42, and 56-59, and col. 10 lines 6-9 and 41-43; ‘452 Patent col. 10 lines 59-62, col. 11 lines 26-29 and 63-66, col. 12 lines 46-49 and 65-68, and col. 13 lines 45-47; ‘781 Patent col. 7 lines 18-21 and 55-58; col. 8 lines 5-8, 27-30, and 64-67, and col. 9 lines 33-36.

During oral argument on the motion for summary judgment, counsel for TecSec argued that “selecting a label is selecting what that label will have on it,” explaining that “[a] user . . . selects all the components that go into a label,” and then the “software creates [the label] based on the user inputs.” MSJ Oral Argument Transcript at 8. Under this argument, “selecting a label” means “selecting the components of the label” because “[t]hat is how software has to work. Software doesn’t work in a vacuum. A user has to tell it what to do.” *Id.* at 8. Adobe responded that merely selecting components of the label is not what the patents describe because the language used is “selecting the label.” *Id.* at 13-14.

Adobe has the better of the argument. The language of claim 1 is clear that the “label” is selected; the claim does not state that the “components of a label” are selected. That distinction is supported by other claims which draw a distinction between the label and the components within the label. For example, claim 8 states that “label conditions” within an “object labelling subsystem” limit object access. If “label” meant the same thing as “label conditions,” one would expect the same term to be used for each. Different terms generally have different meanings. Chicago Bd. Options Exch., Inc. v. Int’l. Secs. Exch., LLC, 677 F.3d 1361, 1369 (Fed. Cir. 2012).

The conclusion that “selecting a label” is different from “selecting the components of a label” is also supported by the written description. Immediately after stating that “a network manager or user can be assured that only those messages meant for a certain person, group of persons, and/or location(s) are in fact received, decrypted, and read by the intended receiver,” the ‘702 Patent states that “[t]hus, a sending user can specify label conditions.” Col. 2 lines 40-46. This language indicates that the label contains conditions on which access is regulated. Additionally, the ‘702 Patent lists components of the object when describing what is

encapsulated, rather than merely stating that the object is encapsulated, col. 8 lines 18-21, thereby supporting the conclusion that if “selecting a label” meant “selecting label components,” the claim would say so.

TecSec’s argument that a piece of software must create the label does not change this result. That a computer must create a label at some point in order for the user to select it does not mean that selecting a label and selecting the components used in its creation are the same thing. Neither does the Court’s construction require a user to somehow reach into a computer and manipulate the electrical data to select a label; it merely requires that the label be chosen from labels which had previously been created. The selection can only occur after the creation, and selection must be of the label itself, rather than the components or conditions which are used to create the label. Accordingly, the phrase “selecting a label” is construed to mean “choosing a pre-existing label,” and does not include selecting the components for the label.¹³

2. “object-oriented key manager”

The term “object-oriented key manager” only appears in the asserted method claims.¹⁴ TecSec argues that the term means “software that controls access to the algorithm used to encrypt and decrypt objects.” Adobe argues that it means “a software component that manages the encryption of an object, on an object-by-object basis, to achieve multi-level security, including the process of generating, distributing, changing, replacing, storing, checking on, and

¹³ As will be explained later, the construction of “selecting” is dispositive on the issue of infringement. Because TecSec and Adobe have vigorously litigated the other claim terms, those terms are also ripe for construction. O2 Micro Intern. Ltd., 521 F.3d at 1362. Resolution of the meaning of those terms will also assist in early resolution of the claims that TecSec asserts against the remaining defendants.

¹⁴ Specifically, those are claims 1 and 4 of the ‘702 Patent, claim 1 of the ‘755 Patent, claim 1 of the ‘452 Patent, and claims 1 and 3 of the ‘781 Patent.

destroying cryptographic keys.” Both Adobe and TecSec draw their definitions from a section of the written description introduced during the prosecution of the ‘702 Patent after a rejection by the examiner. Declaration of Michael A. Oakes [Dkt. No. 737] Ex. 9 (“O.A. Response”) at 11. The examiner had rejected claim 1 (then the only pending claim) under 35 U.S.C. 112 ¶ 2 (now 35 U.S.C. 112(b)) as being indefinite. Id. at 10. One of the terms that the examiner identified as being indefinite was “key manager.” Id. In response, the applicant added the following language to the written description:

Various methods have evolved to manage the distribution of keys. Such methods of distribution are collectively referred to as “key management.” The function of key management is to perform the process of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys. Under normal operational circumstances, the key manager begins and ends a cryptographic session by controlling access to the algorithm used to encrypt and decrypt plain text objects. Thus, a user who wants to encrypt an object or decrypt an object must first access the key manager so that an encryption algorithm may be chosen.

Id. at 1-2. The applicant stated that the language was added “to define key manager and to explain accessing the key manager.” Id. at 11.

Adobe draws its construction from that description by focusing on “the function of key management,” though it adds that the object-oriented key manager “manages the encryption of an object, on an object-by-object basis, to achieve multi-level security.” TecSec draws its construction from how the key manager functions “[u]nder normal operational circumstances.”

TecSec’s proposed construction will be rejected because it does not comport with the language of the claims and the written description. TecSec purports to be defining the term “object-oriented key manager,” but its proposed construction indicates that the “key manager” controls access to an algorithm, not a key. From its plain language, a “key manager” must, at some level, manage a key or keys, and TecSec’s definition does not provide for that. TecSec’s proposed definition also omits a portion of the written description that it purports to quote.

Specifically, TecSec seeks to construe the term as “software that controls access to the algorithm used to encrypt and decrypt objects.” The section from which TecSec draws its definition, however, states that the key manager “control[s] access to the algorithm used to encrypt and decrypt plain text objects.” Col. 2 lines 1-2 (emphasis added).

The intrinsic evidence shows that Adobe’s construction is more accurate. That construction rests on the unstated but reasonable assumption that a “key manager” is a “thing that performs key management.” In defining “key manager,” then, it is appropriate to draw from the definition of “key management” provided by the ‘702 Patent: that “[t]he function of key management is to perform the process of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys.” Col. 1 lines 63-66. The definition in the written description does not provide support for Adobe’s inclusion of the requirement that the key manager “manages the encryption of an object, on an object-by-object basis, to achieve multi-level security.” Accordingly, that clause will not be included.

TecSec argues that the claims of the ‘702 Patent contradict Adobe’s construction because the claims do not reflect all of the functions in Adobe’s definition. That argument fails because an inventor may disclose many different embodiments of an invention in the written description, and may describe many different capabilities of the same embodiment. Although claim 1 of the ‘702 Patent reflects only “the cryptographic functions of encrypting an object and decrypting an object, not distributing or destroying keys,” MSJ Opp’n at 19, that statement does not mean that including the capability to distribute or destroy keys in the claim construction is incorrect; it only means that the inventor of the ‘702 Patent chose, for whatever reason, to focus the claims of that particular patent on a subset of functions of which the object-oriented key manager was capable.

For these reasons, Adobe's proposed definition is modified and the term "object oriented key manager" is construed to mean "a software component that is capable of performing the process of generating, distributing, changing, replacing, storing, checking on, and destroying cryptographic keys." Because the intrinsic evidence in the patent is sufficiently clear and unambiguous, reference to extrinsic evidence is unnecessary.

3. "label"

The term "label" appears in all of the asserted claims. TecSec argues that the term means "an identifier associated with an object," while Adobe argues that it means "a series of letters or numbers, separate from but associated with the sending of an object, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated object and which provides a level of protection in addition to cryptographic protection." Adobe adopts its proposed construction from the '702 Patent, which states that:

A file 'label' for purposes of this invention means a series of letters or numbers, which may or may not be encrypted, separate from but associated with the sending of a message, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated message.

Col. 2, lines 34-40.¹⁵ Because the claims themselves do not include a "message," Adobe replaces "message" with "object," which does appear in the claims, and adds the phrase "and which provides a level of protection in addition to cryptographic protection" because, Adobe argues, "[t]he specifications of the DCOM [P]atents explain that the labels are attached by software to an encrypted object to add a layer of security." MSJ Br. at 21. To support this construction, Adobe again cites the written description of the '702 Patent which provides that "[b]y being able to

¹⁵ This definition also appears in the '755 Patent and the '781 Patent. '755 Patent col. 2 lines 32-38; '781 Patent col. 2 lines 22-28.

compartment every object by label attributes and algorithm attributes, multi-level multimedia security is achieved.” Col. 4 lines 22-25.

In contrast, TecSec argues that its construction of “label” as “an identifier associated with an object” is appropriate because its construction comports with the “ordinary and customary meaning” of the term “label.” TecSec also argues that the “specification does not give [“label”] a special meaning,” and that extrinsic evidence, for example a technical dictionary, supports this “plain meaning.” MSJ Opp’n at 21. TecSec attempts to explain the language quoted by Adobe as simply part of the disclosure of another patent, U.S. Patent No. 5,369,707 (the “’707 Patent”), which was included in the ‘702 Patent as a description of the prior art which the ‘702 Patent sought to replace. The paragraph immediately following the section that Adobe cites for its definition states that “[a] system such as that described above is disclosed in [the patent application which became the ‘707 Patent], filed Jan. 27, 1993, the specification of which is incorporated by reference herein.” ‘702 Patent Col. 2 lines 58-61.

The plain text of the ‘702 Patent shows that TecSec’s argument is incorrect and that Adobe has correctly relied on that section. The written description never uses the word “invention” to apply to anything other than the system described by the ‘702 Patent. At no point does the written description refer to the system described by the application which would become the ‘707 Patent as an “invention;” by contrast, it refers to the system of the ‘702 Patent as “the invention” at least eighteen times.¹⁶ Because the only thing that the written description

¹⁶ See, e.g., col. 1 line 5 (“field of the invention”); col. 1 line 13 (“background of the invention”); col. 3 line 11 (“summary of the invention”); col. 3 lines 12, 18, 21, 25, 29, and 42, col. 4 lines 14, 31, 38, 39-40, 47, 52, col. 5 line 18, col. 11 line 61 (“the present invention”); col. 4 lines 56-57 (“detailed description of the invention”) (emphasis added).

refers to as an “invention” is the system described by the ‘702 Patent, “this invention” must mean “the invention described by the ‘702 Patent.”

The language quoted by TecSec, referring to the ‘707 Patent, does not contradict this result. It is possible, and even common, for inventors to seek patents for different aspects of a single product or technology (for example, TecSec received the four patents at issue by claiming variations of the DCOM system). That a specific definition for “label” was used in the ‘707 Patent does not preclude an inventor from using the same definition in the ‘702 Patent, or a multitude of other patents, as well. Inventors often use terms of art, which have the same definition across an entire field. It is similarly unsurprising that different inventors employed by the same company would use the same definition when applying for a patent. Although TecSec attempts to make much from the fact that the ‘702 and ‘707 Patents have different inventors, the cover pages of the two patents reveal that both patent applications were prepared and prosecuted by the same two individuals.

During oral argument, counsel for TecSec disparaged Adobe’s proposed construction, describing it as drawn from the background of the invention which only functioned to describe the prior art. MSJ Oral Argument Transcript at 16-17. Nothing prevents an inventor from defining a relevant claim term in the background section of the written description. TecSec appears to recognize this fact, as it draws its proposed construction of “object-oriented key manager” from the background section of the ‘702 Patent. See supra.

TecSec’s expert Dr. Jones opined that “the inventor of the ‘702 Patent purposefully distinguished his invention from the [‘707 Patent] . . . and the section relied upon by Adobe is relevant only to the ‘707 [P]atent.” Jones Dec. ¶ 66. That opinion does not change the Court’s analysis because Dr. Jones does not explain the basis for his opinion or why the section relied

upon by Adobe is only relevant to the ‘707 Patent, and fails to provide any evidence to support his opinion. “[T]here must be some foundation or basis” for an expert opinion. Invitrogen Corp., 429 F.3d at 1080. As Dr. Jones’ opinion is not supported by any evidence, other than his bald assertion, the Court accords that opinion little weight in its analysis.

Finally, TecSec argues that the written description of the ‘452 Patent, which describes “label” in more detail¹⁷ (while still bearing a definition similar to that provided in the ‘702 Patent) shows that the DCOM Patents use a different, more flexible, definition of “label” than the definition in the ‘707 Patent. MSJ Opp’n at 22. TecSec’s argument is flawed for several reasons. First, the section of the ‘452 Patent that TecSec cites is entirely consistent with the definition of “label” provided in the ‘702 Patent, ‘755 Patent, and ‘781 Patent – which makes sense, considering that the ‘452 Patent adopts the definition from the ‘702 Patent almost verbatim.¹⁸ ‘452 Patent col. 3 lines 1-7. Moreover, the ‘452 Patent does not have the “system such as that described above” language (referring to the ‘707 Patent) on which TecSec hangs its argument. Lastly, any arguable modification to the definition caused by the ‘452 Patent could not affect the definition in the ‘702 Patent because the application which became the ‘452 Patent was filed after the ‘702 Patent already issued. The evidence, across all of the DCOM Patents, indicates that the inventor intended “label” to have a particular definition as expressed in almost identical terms in each patent. Moreover during the more than five years between the filing of the application that became the first DCOM Patent to the issuance of the last DCOM Patent, TecSec

¹⁷ The ‘452 Patent states that “[a] file ‘label,’ relative to the present invention mean a series of characters, which may or may not be encrypted, separate from the file or message but associated with the storing of a file or the sending of a message, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated message or to read or modify an associated file.” Col. 3 lines 1-7.

¹⁸ See supra n.17.

made no effort to modify the quoted language in any meaningful way. This course of conduct is powerful evidence that the inventor intended a special definition for the term “label,” and not the ordinary meaning that TecSec now seeks.

For the foregoing reasons, by using the language “[a] file label for the purposes of this invention means” the patentee indicated the intent to provide a special definition for the word “label,” rather than the ordinary definition. See Thorner, 669 F.3d at 1366 (quoting with approval a pre-Philips decision finding that the inventor acted as his own lexicographer).

TecSec argues that Adobe’s definition is inappropriate because Adobe replaces the word “message,” which appears in the written description, with “object,” which appears in the claims. MSJ Opp’n at 22. Contrary to TecSec’s arguments, the change of “message” to “object” does not defeat Adobe’s proposed construction. For the reasons explained above, it is clear that the inventor intended a special definition for the term “label” when drafting the ‘702 Patent. “The terms used in patent claims are not construed in the abstract, but in the context in which the term was presented and used by the patentee, as it would have been understood by a person of ordinary skill in the field of the invention on reading the patent documents.” Fenner Investments, Ltd. v. Celco P’ship, 778 F.3d 1320, 1322-23 (Fed. Cir. 2015). The relevant section of the written description defines a “label for purposes of this invention” by reference to a “message.” ‘702 Patent col. 2 lines 31-40. The claims define the invention, however, by reference to an “object.” In light of the inventor’s intent to provide a particular definition for “label” while claiming an invention involving “objects,” “the context in which the term was presented and used by the patentee,” Fenner, 778 F.3d at 1322, indicates that substitution of “object” for “message” is appropriate in the construction of “label.”

TecSec also argues that the phrase “a series of letters or numbers, which may or may not be encrypted, separate from but associated with the sending of an object,” from Adobe’s definition and adapted from the definition in the ‘702 Patent, is “nonsensical” in the context of the claims because “there is no requirement in the claims or the specification of the DCOM Patents that objects must be ‘sent.’” MSJ Opp’n at 22. Importantly, however, the definition does not require actual sending of the object, but only that the label is “associated” with the sending of the object. “Determining access authorization based on the object label” and that the method is “for providing multi-level multimedia security in a data network,” both limitations present in the claims, indicate that the label is “associated” with the sending of the object, as provided in the definition.

TecSec also attacks the last clause of Adobe’s construction of “label,” which states that the label “provides a level of protection in addition to cryptographic protection.” That clause does not appear in the definition in column 2 of the ‘702 Patent, and was added by Adobe because “[t]he specifications of the DCOM patents explain that the labels are attached by software to an encrypted object to add a layer of security.” MSJ Br. at 22. TecSec argues that the added clause appears nowhere in the claims or specification of the ‘702 Patent, and there is nothing inherent in the word “label” that requires it to provide additional protection. MSJ Opp’n at 22. Instead, the label is merely the method through which a subsystem determines whether to allow access. *Id.* at 23.

TecSec has the better of the argument. Although the specification describes the label as being used to provide security in addition to encryption, that feature already appears in the claims. In claim 1, for example, access authorization is determined based on the object label, and the object is only decrypted if access authorization is granted. As the feature already appears in

the claims, there is no basis on which to add it to the construction for “label.” Further, the added clause runs afoul of the same problem as TecSec’s proposed construction – namely, that the inventor provided an explicit definition for the term “label” which does not include the added clause. The inventor may be his own lexicographer, and when he elects to do so his usage will be given effect.

Accordingly, the Court construes the term “label” to mean “a series of letters or numbers, separate from but associated with the sending of an object, which identifies the person, location, equipment, and/or organization which is permitted to receive the associated object.”

4. “labelling”

The term “labelling” appears in all of the asserted claims. TecSec argues that the term means “attaching a label,” and Adobe argues it means “attachment of a label to an object by software after encryption of that object.” Adobe argues that its construction is supported by the written descriptions of the DCOM Patents because the patents provide that labelling produces protection “in addition to cryptographic protection.” Adobe Systems Incorporated’s Reply in Support of its Proposed Claim Constructions and Motion for Summary Judgment of Non-Infringement [Dkt. No. 753] (“Reply Br.”) at 12. TecSec responds that the temporal limitation proposed by Adobe introduces duplicative limitations into the claim terms. MSJ Opp’n at 23-24. For example, claim 1 requires “labelling the encrypted object” which means that labelling necessarily occurs after encryption of the object. Although the particular implementation of claim 1 requires labelling after encryption, there is nothing in the specification which requires all labelling to occur after encryption. See col. 2 lines 31-57. Accordingly, TecSec’s construction of the term “labelling” to mean “attaching a label” is the proper construction.

5. “access authorization”

The term “access authorization” appears in all of the asserted method claims.¹⁹ TecSec argues the term means “authorization to access an object,” while Adobe argues that it means “authorization to access an object with particular permissions based on the identity of the accessing entity rather than a password.” Adobe argues that its construction is supported by other terms in the asserted claims because the “plain claim language dictates that ‘access authorization’ is based on the object label.” MSJ Br. at 24 (emphasis removed). In essence, Adobe reads its construction of “label” into “access authorization.” Adobe does not cite any section of the DCOM Patents to support its proposed construction. See id. at 24-25. TecSec responds that the claim term “is written in plain English that would be well-understood by a person of ordinary skill in the art when read in light of the” DCOM Patents and that the language of the claim requires access authorization based on a label, “any construction of the term ‘label’ is present in the claim language.” MSJ Opp’n at 27.

Adobe’s construction of “access authorization” is too restrictive. The plain language of the claims requires access authorization “based on the object label,” and the Court has construed a “label” to identify the “person, location, equipment and/or organization which is permitted to receive the associated object.” Adobe seeks to introduce into the construction of “access authorization” the requirement that the authorization is “based on the identity of the accessing entity.” To the extent that “identity” is simply a reflection of the “person, location, equipment, and/or organization” language, imposing that requirement is duplicative of the “label” construction because the plain language of the claims requires that access authorization be

¹⁹ Specifically, in claims 1 and 4 of the ‘702 Patent, claim 1 of the ‘755 Patent, claim 1 of the ‘452 Patent, and claims 1 and 3 of the ‘781 Patent.

granted “based on the label” – i.e., based on the person, location, equipment, and/or organization which is permitted to receive the associated object. Any definition of “access authorization” narrower than the definition of “label” would contradict the language of the claims, which specifically states that access authorization is based on the label. In either case, Adobe’s construction of “access authorization” is not appropriate.

The ‘702 Patent does not give any special meaning to the term “access authorization.” Accordingly, the term is construed in accordance with its ordinary meaning to be “authorization to access an object.”

6. “display” / “displaying”

The term “displaying” appears in claim 1 of the ‘452 Patent, and the term “display” appears in claim 1 of the ‘755 Patent (through reference to a “display header”). Adobe argues that both terms should be construed to mean “making visually perceptible to a user.” MSJ Br. at 25. Adobe argues that its construction is correct in light of the Summary of the Invention of the ‘452 Patent, which states that “[t]he label may appear as a header to authorized users. . . . For example, the header may identify the object as a container object, and may further list the objects embedded in the container object, preferably in the form of an array, or tree structure.” Id. (quoting ‘452 Patent col. 6 lines 7-13). TecSec responds that Adobe’s construction is unnecessary because the terms are easily understandable and so should be given their plain and ordinary meaning, and that Adobe’s “one size fits all” definition does not match the use of “display” (as part of the term “display header”) in the ‘755 Patent. MSJ Opp’n at 28-29.

“Display” and “displaying” cannot be given the exact same construction because the two terms are different parts of speech. In the context of the claims at issue, “display” is an adjective modifying “header,” and “displaying” is a verb. There is no evidence that the inventor intended

to act as his own lexicographer and provide a special definition for those terms. Accordingly, those terms will be given their plain and ordinary meaning. The plain and ordinary meaning is “the meaning [that the term] would have to persons in the field of the invention, when read and understood in light of the entire specification and prosecution history.” Fenner, 778 F.3d at 1323 (citing Phillips, 415 F.3d at 1312-17). Adobe argues that its own definition is the “ordinary meaning of display.” MSJ Br. at 25. TecSec does not propose its own definition, and does not dispute that Adobe’s proposed construction is consistent with the ordinary meaning. See MSJ Opp’n at 25-26. Accordingly, “displaying” is construed to mean “making visually perceptible to a user.” As “display” is used as an adjective in the context of the ‘755 Patent’s “display header” term, “display” is construed together with “header” to mean “a header for making visually perceptible to a user.”

C. Infringement

Remaining before the Court is Adobe’s motion that it should be granted summary judgment on TecSec’s claim that Acrobat directly infringes the DCOM Patents.²⁰ “To prove direct infringement, the plaintiff must establish by a preponderance of the evidence that one or more claims of the patent read on the accused [product] literally or under the doctrine of equivalents.” Cross Med. Prods., Inc. v. Medtronic Sofamor Danek, Inc., 424 F.3d 1293, 1310 (Fed. Cir. 2005). To prove direct infringement of a method claim, “a patentee must prove that

²⁰ Adobe originally presented argument regarding divided and indirect infringement, see MSJ Br. at 26-29, but those issues were struck from consideration on TecSec’s motion. November 14, 2014 Order [Dkt. No. 728]. At oral argument on the motion to strike, counsel for TecSec admitted that if Acrobat does not directly infringe the DCOM Patents, then Adobe does not infringe under any other theory of infringement. Transcript of November 14, 2014 Hearing [Dkt. No. 745] at 6-7. Adobe also argues that it does not infringe the asserted system claims because Adobe does not sell computer hardware, MSJ Br. at 27-28; that argument was previously dismissed on November 14, 2014. [Dkt. No. 728].

each and every step of the method or process was performed.” Aristocrat Techs. Australia Pty. Ltd. v. Int’l Game Tech., 709 F.3d 1348, 1362 (Fed. Cir. 2013).

TecSec and Adobe present argument regarding whether Acrobat performs multiple claim terms; however, because failure to generate a genuine issue of material fact on a single claim term precludes a finding of infringement as a matter of law, the Court will only address a subset of those arguments.

1. Multi-level Encryption

Adobe claims that it should be granted summary judgment on TecSec’s claim that Acrobat performs multi-level encryption because TecSec has not created a genuine issue of material fact regarding whether Acrobat performs that function. In response, TecSec has provided evidence that Acrobat can perform multi-level encryption by the following steps: (1) the user opens a first PDF document using a first session of Acrobat; (2) the user selects the encryption conditions for the first PDF document; (3) the user saves the first PDF document to create a first encrypted PDF document; (4) the user creates a second PDF document using a second session of Acrobat; (5) the user attaches the first encrypted PDF document to the second PDF document; (6) the user selects the encryption conditions for the second PDF document (which has the encrypted first PDF document attached); and (7) the user saves the second PDF document, thereby nesting the first encrypted PDF document within the second encrypted PDF document. MSJ Opp’n at 12-16.

Adobe claims that TecSec’s argument is defeated by the fact that multiple sessions of Acrobat must be used for Acrobat to operate in the manner described by TecSec. Reply Br. at 7-8. Adobe does not cite to any precedent for its seemingly novel argument that a computer program only infringes a patent if it performs all of the elements of a claim in a single session of

that program. See id. TecSec has not accused a single session of Acrobat of infringing the DCOM Patents, but instead has accused the Acrobat program of infringement. Not only has TecSec presented evidence that Acrobat could be used to perform multi-level encryption, Kaufman 30(b)(6) Dep. at 70-72; Oakes Dec. Ex. 6-7, TecSec has also presented evidence that Adobe has instructed its customers that Acrobat could be used in that manner. Oakes Dec. Ex. 5. Specifically, Adobe posted to its website, and therefore instructed its users, that

If you want to send multiple documents together in a PDF envelope, and you want those PDF attachments to retain their protections after the outer PDF envelope is opened – then you should protect the PDF files individually before they are attached. You then have an option of encrypting the outer PDF envelope hosting the attachments.

Id. This provides evidence that use of multiple sessions to provide multiple layers of encryption was an intended, rather than unforeseen, use of Acrobat. In sum, TecSec has provided sufficient evidence that Adobe has informed its customers that Acrobat could be used in a manner which provides multi-level encryption, and has instructed those customers how to do so. This evidence defeats Adobe's motion for summary judgment on this issue.

2. Whether the Encryption Dictionary is a Label

Adobe argues that Acrobat's encryption dictionary is not a "label" as defined by the DCOM Patents because the encryption dictionary "does not identify a person, a location, equipment, or an organization" as required by the DCOM Patents, and therefore summary judgment of non-infringement is appropriate. MSJ Br. at 23.²¹ TecSec responds that the encryption dictionary is a label both when the PDF document is secured using a password and when the PDF document is secured using certificates. MSJ Opp'n at 24-25. Specifically, when

²¹ Adobe also argues that TecSec disclaimed use of passwords during prosecution of the '702 Patent. MSJ Br. at 19. Even if TecSec did not disclaim the use of passwords, Acrobat still does not infringe as a matter of law and therefore Adobe's disclaimer argument need not, and will not, be addressed.

using password security, the password identifies the user and when using digital certificates, the encryption dictionary contains information which identifies the owner of the relevant digital certificates. Id. at 25.

Adobe has the better of the argument regarding password security. As explained previously, the encryption dictionary does not contain either the user or owner passwords. Kaufman 30(b)(6) Dep. at 17. Instead, the encryption dictionary contains an “O key” and “U key” used to test the information entered by the user to see if the user entered the correct password. Id. Even if the encryption dictionary included the actual user and owner passwords Adobe would still have the better of the argument because under Acrobat’s system, the user and owner passwords are not linked to the identity of a particular user. Like a housekey, anyone’s possession of the password grants access. The password is simply a talisman which grants access irrespective of the identity of the person using it. When using password security, the encryption dictionary does not identify any person, location, equipment, or organization and therefore the encryption dictionary does not constitute a label when password security is used. Accordingly, Adobe’s prevails on the argument that the encryption dictionary is not a label when password security is used.

In contrast, TecSec has presented evidence that the encryption dictionary is a label when digital certificates are used because the encryption dictionary contains identifiers for the digital certificates related to the public keys used to encrypt the file key. Id. at 52-54. This finding is supported by Mr. Kaufman who, when asked if “the certificate IDs identify each of the individual recipients,” responded “[y]es.” Id. at 54. Therefore, TecSec has presented sufficient evidence that, when using certificate security, the encryption dictionary identifies the person who

is permitted to receive the associated object, thereby defeating Adobe's argument that the encryption dictionary is not a label when certificate security is used.

3. Selecting a Label

Every claim at issue contains either "selecting a label" or "selecting a first label" as an element.²² Under the Court's construction of "selecting a label," the label must exist before it can be selected. Therefore, the element of "selecting a label" means that the label itself, not the conditions of the label, must be selected.

TecSec argues that the encryption dictionary generated by Acrobat and inserted into the trailer section of a PDF document as part of the encryption process is the "label" required by the claims. MSJ Opp'n at 24. As previously explained, the encryption dictionary qualifies as a label under the Court's construction only when certificate security is used.

Even if TecSec's view of the encryption dictionary generated by Acrobat as the label was accepted, TecSec has not raised a genuine dispute of material fact establishing that Acrobat performs the required "selecting" step because it is undisputed that a user of Acrobat does not select the encryption dictionary (TecSec's "label"). MSJ Opp'n at 24; Kaufman 30(b)(6) Dep. at 35, 54, 63; MSJ Oral Argument Transcript at 6 ("The user doesn't create the label."). Under the Court's construction of "selecting a label," the label itself must be selected, not created, which under TecSec's argument means that the encryption dictionary (TecSec's label) must be selected;

²² All asserted method claims include the "selecting" language, and all system claims include selection through the "object labelling subsystem" and "object label identification subsystem," which restrict access based on "label conditions" present in a selected label. Because the claims use only "slightly different language to describe substantially the same invention," they will be treated the same. Ohio Willow Wood Co. v. Alps South, LLC, 735 F.3d 1333, 1342 (Fed Cir. 2013). Moreover, the parties have grouped all asserted claims together for the purposes of the motion for summary judgment, any argument that they should be treated differently is deemed waived. Voter Verified, Inc. v. Premier Election Solutions, Inc., 698 F.3d 1374, 1382 (Fed. Cir. 2012).

however, as explained above in Section I.D, the encryption dictionary is automatically generated by Acrobat when the user elects to “save” the document. Given the un rebutted evidence of how Acrobat generates the encryption dictionary, Acrobat does not meet the “selecting a label” element. Therefore, Adobe is entitled to summary judgment of non-infringement.

Even if TecSec were correct that selecting the conditions for a label is the same as selecting a label, it remains undisputed that the encryption dictionary does not exist when the conditions of the label are selected; instead, the encryption dictionary is not created until the user saves the file. Kaufman 30(b)(6) Dep. at 35, 54, 63. Under the Court’s construction, the label must be created before it can be selected. In other words, in Acrobat the encryption dictionary (TecSec’s label) does not exist when the user selects the various conditions for access to the object. It is not until the user saves the document that the encryption dictionary (TecSec’s label) comes into existence. Accordingly, under this Court’s construction of “selecting,” Acrobat does not infringe, and Adobe’s motion for summary judgment of non-infringement will be granted.²³

4. Doctrine of Equivalents

TecSec argues that even if Acrobat does not literally infringe the claims of the DCOM Patents, Acrobat infringes under the doctrine of equivalents. MSJ Opp’n at 30. “Even without literal infringement of a certain claim limitation, a patentee may establish infringement under the doctrine of equivalents if an element of the accused device ‘performs substantially the same

²³ Although not briefed by the parties, there are other aspects of the DCOM Patents that Acrobat does not perform. For example, each asserted claim requires some form of “labelling.” At TecSec’s urging, “labelling” has been construed to mean “attaching a label.” Acrobat does not attach an encryption dictionary to an encrypted PDF document; instead, it inserts the encryption dictionary into the (pre-existing) trailer for that file. Jones Dec. ¶ 68. Indeed, far from being attached to the encrypted object, “[t]he encryption dictionary is part of the trailer portion of a PDF document.” *Id.* Thus, what TecSec alleges is a label is not “attached to” the object, it is part of the object.

function in substantially the same way to obtain the same result as the claim limitation.” EMD Millipore Corp. v. AllPure Techs., Inc., 768 F.3d 1196, 1202 (Fed. Cir. 2014) (quoting AquaTex Indus., Inc. v. Techniche Solutions, 419 F.3d 1374, 1382 (Fed. Cir. 2005)). To support a finding under the doctrine of equivalents, a patentee must “provide particularized testimony and linking argument as to the insubstantiality of the differences between the claimed invention and the accused device or process, or with respect to the function, way, result test . . . Such evidence must be presented on a limitation-by-limitation basis.” W.L. Gore & Assocs., Inc. v. Medtronic, Inc., 874 F. Supp. 2d 526, 542 (E.D. Va. 2012). TecSec argues that it has provided the required analysis in its infringement contentions; however, TecSec’s contentions are not supported by any evidence, such as an expert declaration, establishing that the differences between Acrobat and the DCOM Patents are insubstantial, or that Acrobat performs the same function as the DCOM Patents, in the same way, to reach the same result. Accordingly, TecSec’s doctrine of equivalents argument fails as a matter of law.

5. Liability After October 20, 2013

Adobe argues that because the DCOM Patents expired on October 20, 2013, Adobe does not have any potential liability after that date. MSJ Br. at 28; Reply Br. at 20. TecSec does not contest that argument, see MSJ Opp’n, which is correct as a matter of law. Kearns v. Chrysler Corp., 32 F.3d 1541, 1550 (Fed. Cir. 1994) (“[T]here can be no infringement once the patent expires.”). Accordingly, Adobe’s Motion for Summary Judgment that it is not liable for any allegedly infringing acts occurring after October 20, 2013 will also be granted.


IV. CONCLUSION

For the reasons stated above, defendant Adobe Systems Incorporated’s Motion for Entry of its Proposed Claim Constructions and for Summary Judgment of Non-Infringement. [Dkt. No.

710] will be GRANTED IN PART as to its claim constructions and GRANTED as to summary judgment of non-infringement by an appropriate Order to be issued with this Memorandum Opinion.

Entered this 7th day of May, 2015.

Alexandria, Virginia

/s/ 

Leonie M. Brinkema
United States District Judge